

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Western District of Wisconsin

In the Matter of the Search of)
 N6960 Bice Ave, Holmen, LaCrosse County, Wisconsin;) Case No. 24-mj-5
 2018 gray Tesla Model 3 with WI registration plate 830-)
 NLZ; silver 2017 Subaru Crosstrek SUV with WI)
 registration plate 178-TNW; the person of Steven Anderegg)

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following premises located in the Western District of Wisconsin.

See Attachment A.

The person or property to be searched, described above, is believed to conceal:

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the information described in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 3-5-24 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

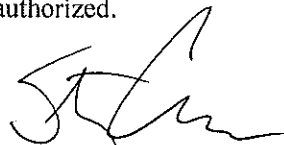
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Stephen L. Crocker or United States Magistrate Judge Andrew R. Wiseman.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for Days delayed days (not to exceed 30)
☐ until, the facts justifying, the later specific date of Date ending.

☐ Entry without knocking and announcing authority and purpose authorized.

Date and time issued:

2-20-24 AT 3:15 PM


Judge's signature

Madison, Wisconsin

Magistrate Judge Stephen L. Crocker
 Magistrate Judge Andrew R. Wiseman

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

24-mj-5

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

ATTACHMENT A

1. The property to be searched is N6960 Bice Ave, Holmen, LaCrosse County, Wisconsin further described as a two-story, single-family residence on the east side of the street that faced to the west. The residence had an attached three car garage. The house is covered in a mix of light tan horizontal vinyl siding and light brown/gray brick. The lower third of the garage pillars and entire front porch area have the same brick. The front door is tan and has a thin vertical window to the left of the door. The top of the door has a window shaped in a half-circle. Affixed horizontally to the brick on the pillar to the right of the garage are the numbers "N6960." At the end of the driveway is a green sign affixed to a metal post with the numbers on "N6960" vertically. The roof appears to have brown asphalt shingles. There appears to be one storage shed visible from the road on the property. The shed is located south of the residence and was brown in color.
2. The vehicles to be searched are a 2018 gray Tesla Model 3 with Wisconsin registration plate 830-NLZ and a silver 2017 Subaru Crosstrek SUV with Wisconsin registration plate 178-TNW, both returning to Anderegg's residence.
3. According to Anderegg's driver's license, he is 6'2", weighs 220 pounds, and has brown hair and blue eyes.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography, child erotica, or visual representations of any kind of minors engaged in sexually explicit conduct; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, visual representations of any kind of minors engaging in sexually explicit conduct, or information pertaining to an interest in child pornography, child erotica, or any such visual representations.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the distribution or possession of child pornography, the production, distribution, or possession of explicit material in violation of 18 U.S.C. §1466A, transferring or attempting to transfer obscene material to a minor in violation of 18 U.S.C §1470, or the importation or transportation of obscene matter in violation of 18 U.S.C. §1462(a).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of N6960 Bice Ave, Holmen, WI, by use of the computer or by other means for the purpose of distributing or receiving in any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or visual depictions of any kind of minors engaged in sexually explicit conduct, or that cater to those with an interest in child pornography or such depictions.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography or visual depictions of any kind of minors engaging in sexually explicit conduct to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts

with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (electronic storage device) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;
- e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that

are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Western District of Wisconsin

In the Matter of the Search of
 N6960 Bice Ave, Holmen, LaCrosse)
 County, Wisconsin; 2018 gray Tesla Model)
 3 with WI registration plate 830-NLZ;)
 silver 2017 Subaru Crosstrek SUV with WI)
 registration plate 178-TNW; the person of)
 Steven Anderegg)

Case No. 24-mj-5

SEALED

APPLICATION FOR A SEARCH WARRANT

I, AUSA Elizabeth Altman, an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following premises:
 See Attachment A.

located in the Western District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1466A	Production, distribution, or possession of explicit material
18 U.S.C. § 1462(a)	Importation or transportation of obscene matter
18 U.S.C. § 1470	Transferring or attempting to transfer obscene material to a minor
18 U.S.C. § 2252A	Distribution or possession of child pornography

The application is based on these facts: See attached Affidavit.

☐ Delayed notice of Days delayed days (give exact ending date if more than 30 days: Date ending) is requested under 18 U.S.C. § 3103a, the basis of which is set forth in the attached affidavit.

Applicant's signature

AUSA Elizabeth Altman

Printed name and title

Sworn to before me telephonically on

Date:

2-20-24



Judge's signature

Madison, Wisconsin

Magistrate Judge Stephen L. Crocker
 Magistrate Judge Andrew R. Wiseman

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Condon, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Wisconsin Department of Justice and have been since September of 2016. I have received more than 500 hours of training in the investigation of computer-facilitated exploitation of children, and methods of forensic analysis of computers used in criminal activity. This training was provided by the Wisconsin Division of Criminal Investigation (DCI) and the United States Department of Justice Internet Crimes Against Children (ICAC) Training and Technical Assistance Program. I have written more than 100 search warrant and subpoena applications over my law enforcement career.

2. I am conducting an investigation of Steven A. Anderegg, who is suspected of violating Title 18, United States Code, Sections §§1470, 1462(a), 1466A, and 2252A. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider to be truthful and reliable.

3. Based upon the information described below, I submit that probable cause

exists to believe that Steven A. Anderegg has committed the crimes of Transferring or attempting to transfer obscene material to a minor, in violation of Title 18, United States Code, Section §1470, Distribution or possession of Child Pornography, in violation of Title 18, United States Code, Section §2252A, Production, distribution, or possession of obscene visual representations of the sexual abuse of minors, in violation of Title 18, United States Code, Section §1466A, Importation or transportation of obscene matter, in violation of Title 18, United States Code, Section §1462(a), and that evidence relating to these crimes can be found at N6960 Bice Ave, Holmen, LaCrosse County, Wisconsin (the SUBJECT PREMISES), in his vehicles, a 2018 gray Tesla Model 3 with Wisconsin registration plate 830-NLZ and a silver 2017 Subaru Crosstrek SUV with Wisconsin registration plate 178-TNW, and on his person, all more particularly described in Attachment A of this affidavit, for the evidence more particularly described in Attachment B.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. §§ 1462(a), 1466A, 1470, and 2252A.

a. 18 U.S.C. § 1462(a) prohibits a person from using any interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934), for carriage in interstate or foreign commerce any obscene, lewd, lascivious, or filthy

book, pamphlet, picture, motion-picture film, paper, letter, writing, print, or other matter of indecent character;

b. 18 U.S.C. § 1466A(a) and (b) prohibit a person from knowingly producing, distributing, receiving, possessing with intent to distribute, or possessing a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that depicts a minor engaged in sexually explicit conduct and is obscene or that depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex and lacks serious literary, artistic, political, or scientific value, or attempting or conspiring to do so, where: any communication involved in or made in furtherance of the offense is communicated or transported by the mail, or in interstate or foreign commerce by any means, including by computer, or any means or instrumentality of interstate or foreign commerce is otherwise used in committing or in furtherance of the commission of the offense; any communication involved in or made in furtherance of the offense contemplates the transmission or transportation of a visual depiction by the mail, or in interstate or foreign commerce by any means, including by computer; any person travels or is transported in interstate or foreign commerce in the course of the commission or in furtherance of the commission of the offense; any visual depiction involved in the offense has been mailed, or has been shipped or transported in interstate or foreign commerce by any means, including by computer, or was produced using materials that have been mailed, or that have been shipped or transported in interstate or foreign commerce by any means, including by computer; or the offense is

committed in the special maritime and territorial jurisdiction of the United States or in any territory or possession of the United States;

c. 18 U.S.C. § 1470 prohibits a person from using the mail or any facility or means of interstate or foreign commerce to knowingly transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempting to do so;

d. 18 U.S.C. § 2252A(a)(2) and (b)(1) prohibit a person from knowingly receiving or distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempting or conspiring to do so;

e. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing, or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempting or conspiring to do so;

f. 18 U.S.C. § 2256(2)(A) defines “sexually explicit conduct” to mean actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibit of the anus genitals, or pubic area of any person;

g. 18 U.S.C. § 2256(5) defines “visual depiction” to include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format; and

h. 18 U.S.C. § 2256(8) defines “child pornography” to mean any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

DEFINITIONS

6. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Cellular telephone” or “cell phone” means a handheld wireless

device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual

depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer Server" or "Server," is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

g. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other

memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

l. “File Transfer Protocol” (FTP) is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. “Host Name” is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

n. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

o. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

p. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

q. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

r. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even

very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

s. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

t. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

u. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage

device).

v. "Secure Shell" (SSH) is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

w. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

x. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

y. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

z. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

7. I have consulted in this matter with lay persons and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. I have consulted with Digital Forensic Examiner Ryan Rickaby, who received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner. DFE Rickaby has been a forensic computer examiner with the WI DOJ since 2022. DFE Rickaby has participated in the execution of numerous search warrants and search and seizure operations. DFE Rickaby has informed me that to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To effect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

8. Based on my knowledge, I know that computer and other electronic

device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;

b. the objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. the objects may be contraband or fruits of the crime.

9. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person " deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of

deleted data in a swap or a recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. Based on actual inspection of other evidence related to this investigation, personal photos shared by victims during trips, documents, financial records, I am aware that electronic storage device equipment was used to generate, store, and print documents used in this case. Thus, there is reason to believe that there is an electronic storage device system currently located at the proposed search location.

10. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

11. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection

programs) can indicate who has used or controlled the electronic storage device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculcating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculcate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user’s state of

mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

12. The warrant I am applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

13. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

14. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

15. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Samsung allows users to use Face recognition to unlock mobile phones and other devices. During the Face recognition registration process, the user holds the device in front of his or her

face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face recognition on Samsung devices.

16. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

17. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

18. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode

or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

19. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

20. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know

with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

21. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE,
DISTRIBUTE, OR POSSESS VISUAL DEPICTIONS OF MINORS ENGAGED IN
SEXUALLY EXPLICIT CONDUCT**

22. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics

common to individuals who utilize the internet to advertise, distribute, or possess visual depictions of minors engaged in sexually explicit conduct:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including images, videos, or other visual media.

Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain copies of material depicting minors engaged in sexually explicit conduct in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain such visual depictions for many years.

d. Likewise, such individuals often maintain their images of minors engaged in sexually explicit conduct in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view these images, which are valued highly.

Some of these individuals also have been found to download, view, and then delete visual depictions of minors engaged in sexually explicit conduct on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted material, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other distributors/possessors of such material, conceal such correspondence as they do their sexually explicit material, and often maintain lists of contact information for individuals with whom they have been in contact and who share the same interests in visual depictions of minors engaging in sexually explicit conduct.

g. Such individuals prefer not to be without their visual depictions of minors engaged in sexually explicit conduct for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of CSAM throughout the world.

h. I submit that probable cause exists to believe that a resident of the SUBJECT PREMISES described in Attachment A – Steven A. Anderegg – is the user of the Instagram accounts described below, and that this individual has a demonstrated sexual interest in minors. Specifically, as further described below, there is probable cause to believe that Anderegg is producing, distributing, and possessing obscene

visual depictions of minors engaging in sexually explicit conduct; sending such obscene visual depictions to minors; and has previously downloaded visual depictions of minors engaged in sexually explicit conduct over an online peer-to-peer network. Accordingly, there is probable cause to believe that a resident of the SUBJECT PREMISES likely displays characteristics common to individuals who produce, advertise, distribute, and possess visual depictions of minors engaged in sexually explicit conduct.

**BACKGROUND ON THE NATIONAL CENTER FOR
MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE**

23. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

24. In addition to reports from the general public, reports are made by U.S. electronic service providers, which are required by U.S. federal law to report "apparent child pornography" to NCMEC via the CyberTipline (18 U.S.C. § 2258A) if they become aware of the content on their servers. Leads are reviewed by specially trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the

gathered information to the appropriate law enforcement agency for review and possible investigation.

25. The CyberTipline receives reports, known as CyberTipline reports, on the following type of criminal conduct: possessing, manufacturing, and distributing child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

26. The CyberTipline reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic service provider uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the Internet Protocol (IP) Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. *See* 18 U.S.C. § 2258A(b).

PROBABLE CAUSE

27. On Wednesday, November 8, 2023, I reviewed two CyberTipline reports received by NCMEC. The two reports were filed by Meta Platforms, which owns Instagram and Facebook, on October 12, 2023 (CyberTipline Report 176167714) and

October 18, 2023, CST (CyberTipline Report 176484452). Meta Platforms reported that on or about October 8, 2023, one of the accounts (ACCOUNT 1) distributed what appears to be Artificial Intelligence (AI) images depicting child sexual abuse material (CSAM) through an Instagram direct message to an account belonging to a juvenile.¹

28. According to the information provided by Meta in CyberTipline report 176484452, the account details for ACCOUNT 1 are as follows:

Instagram Full Name: Dom
Instagram Username: dhyanax4dxm
Instagram UID: 60857847038
DOB: June 19 2000
Age: 23
Gender: Male
Associated E-Mail Address: None
Associated Phone Number: None

29. Meta also reported that ACCOUNT 1 had already posted numerous apparent AI images of minimally clothed minor boys or minor boys in bondage attire in August and September 2023, and that the user of ACCOUNT 1 follows another Instagram user whose biography states ".....great to meet on telegram and talk about young boy addiction !!"

30. According to information provided by Meta, the recipient of the apparently AI-generated CSAM was a 16-year-old boy (Minor A).²

¹ Artificial intelligence (AI) is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

² As noted below, law enforcement determined he was actually 15 years old.

31. Meta also provided an excerpt of the Instagram conversation in which ACCOUNT 1 distributed the apparent AI images to the juvenile. The details of the chat are as follows:

Username	Date/Time	Message
Minor A	09/26/23 2:46 p.m. PDT	Hey
dhyanax4dxm (IGID 60857847038)	09/26/23 5:59 p.m. PDT	Hey
Minor A	09/27/23 4:38 p.m. PDT	How are you?
dhyanax4dxm (IGID 60857847038)	09/27/23 7:51 p.m. PDT	Ok I guess?
Minor A	09/28/2023 4:25 a.m. PDT	How old are you?
Dhyanax4dxm (IGID 60857847038)	09/28/2023 9:05a.m. PDT	Slightly old, why?
Dhyanax4dxm (IGID 60857847038)	09/28/2023 9:05 a.m. PDT	Who are you?
Minor A	09/28/2023 1:14 p.m. PDT	I was just wondering, my name is [Minor A]
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:14 p.m. PDT	Hi [Minor A]
Minor A	09/28/2023 1:15 p.m. PDT	Hey Dom
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:15 p.m. PDT	So what's up?
Minor A	09/28/2023 1:16 p.m. PDT	Nothing much, I was just wondering like who you were and how you got those kinds of pictures
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:17 p.m. PDT	Im no one in particular all the images I post are my creations
Minor A	09/28/2023 1:17 p.m. PDT	Like you make them? Or are they AI generated
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:20 p.m. PDT	Yes, they are made with stable diffusion. ³ I create them in so far

³ Based on my training, experience, and discussion with other law enforcement agents and personnel involved with similar investigations, I am aware that Stable Diffusion refers to an AI product or model that allows users to generate detailed images based on user-inputted textual descriptions or prompts. User prompts can include multiple sentences and can provide detailed instructions on the subject, content, setting, level of realism, and references that a user wishes to see in a generated image. Users can also utilize Stable Diffusion to alter an existing image based on similar user-inputted textual descriptions or prompts. The code for Stable Diffusion is open sourced, which generally means that users can use and modify the product without any restrictions.

		as I craft the prompts and control parameters of the ai nets
Minor A	09/28/2023 1:21 p.m. PDT	Ohh okay
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:23 p.m. PDT	Don't hesitate to ask anything else, I'm kinda bored at the moment been a long day so far
Minor A	09/28/2023 1:26 p.m. PDT	That's fair, I just got home from school about half an hour ago
dhyanax4dxm (IGID 60857847038)	09/28/2023 1:44 p.m. PDT	So, what you up to now?
Minor A	09/28/2023 2:15 p.m. PDT	Just kinda hanging out
Minor A	10/04/2023 7:46 p.m. PDT	How often do you post?
Dhyanax4dxm (IGID 60857847038)	10/04/2023 8:1 p.m. PDT	Varies a lot, haven't posted a while since telegram for banned and several of my posts were flagged
Minor A	10/04/2023 8:31 p.m. PDT	Ohh okay
Minor A	10/04/2023 8:31 p.m. PDT	Stable Diffusion can make up a lot of those kinds of pictures and stuff too
Minor A	10/04/2023 8:32 p.m. PDT	It's on pc
dhyanax4dxm (IGID 60857847038)	10/04/2023 8:40 p.m. PDT	I know, that's what I use to generate these images
Minor A	10/04/2023 8:41 p.m. PDT	Ohh that makes sense
dhyanax4dxm (IGID 60857847038)	10/04/2023 8:44 p.m. PDT	So how old are you? Forgot to ask after you asked me
dhyanax4dxm (IGID 60857847038)	10/04/2023 8:54 p.m. PDT	Let me know if you have any special requests. Im bored and looking for inspiration so you might get a custom set
Minor A	10/05/2023 4:47 a.m. PDT	I'm 15
Minor A	10/05/2023 4:48 a.m. PDT	Boys in the woods?
Dhyanax4dxm (IGID 60857847038)	10/05/2023 6:23 a.m. PDT	What are the boys in the woods doing?
Minor A	10/05/2023 6:25 a.m. PDT	Idk talking, hanging out, playing
dhyanax4dxm (IGID 60857847038)	10/05/2023 6:53 a.m. PDT	What age boys?
Minor A	10/05/2023 11:46 a.m. PDT	Pre teen so 12ish
Minor A	10/05/2023 7:02 p.m. PDT	What are they wearing?
Dhyanax4dxm (IGID 60857847038)	10/05/2023 8:16 p.m. PDT	◆
dhyanax4dxm (IGID 60857847038)	10/05/2023 8:16 p.m. PDT	◆
Minor A	10/06/2023 4:25 a.m. PDT	Okay

dhyanax4dxm (IGID 60857847038)	10/06/2023 11:20 a.m. PDT	Sorry bro, life got busy for me, got a couple cooking up for you now
Minor A	10/06/2023 11:45 a.m. PDT	You're good

[...]

dhyanax4dxm (IGID 60857847038)	10/06/2023 12:35 p.m. PDT	Funny if you view in order you see me playing with different models, prompts, settings
Minor A	10/06/2023 12:43 p.m. PDT	Cool!
Minor A	10/06/2023 12:44 p.m. PDT	Yeah that's dope
dhyanax4dxm (IGID 60857847038)	10/07/2023 7:36 p.m. PDT	Few more for ya
dhyanax4dxm (IGID 60857847038)	10/07/2023 7:36 p.m. PDT	This content showing apparant CSAM has been reported to NCMEC and received the following cybertip: 176167714
Minor A	10/07/2023 8:28 p.m. PDT	Preciate it
Minor A	10/09/2023 9:45 a.m. PDT	The 3 to last one is my favorite

32. As shown in the excerpt above, at approximately 7:36 p.m. PDT on October 7, 2023, ACCOUNT 1 distributed content flagged by NCMEC as "apparent CSAM," which was reported to NCMEC by Meta Platforms and documented in CyberTipline report 176167714. I have reviewed that report as well. It contains, among other things, two images that ACCOUNT 1 sent in the above Instagram direct-message conversation. According to CyberTipline report 176167714, the images were viewed by Instagram prior to their submission to NCMEC, and they depict the following:

7FAN2cLkeMP2xxPn387320722_806770904522930_6064114663473091_139_o.jpg
This image depicted what appeared to be a prepubescent juvenile male kneeling on a blue blanket in a wooded area. The male was partially clothed, only wearing a baseball cap and white underwear. The male had his erect penis exposed through the opening in his underwear. In the background of the image were other clothed, pre or young pubescent children. The male was posed in a manner that made his erect penis the focal point of the image. This image appears to be computer-generated content.

mCzQ7MseP4li6GPt384857462_616757293728570_2765743605773120 647_o.jpg

This image depicted what appeared to be a different prepubescent juvenile male kneeling on a blue blanket in a wooded area leaning back on his hands with his legs spread far apart exposing his erect penis. The male had a blue cloth draped across his stomach, but other than that, was completely nude. There was a partially clothed juvenile female with brown hair kneeling to the left of the male looking over his shoulder at him. The male in this image was posed in a manner that made his penis the focal point of the image. This image appears to be computer-generated content.

33. According to Instagram, those two images were uploaded on October 7, 2023, at 9:36 p.m. CST and 9:35 p.m. CST, respectively, by ACCOUNT 1, utilizing IP address 147.219.156.74. Instagram also advised that there was a login to ACCOUNT 1 utilizing that same IP address on October 1, 2023, at 9:08 p.m. CST.

34. Law enforcement determined that this IP address resolved to Charter Communications. On October 20, 2023, as part of this investigation, WI DOJ-DCI Program Policy Analyst (PPA) Jessica Cattaneo requested an Administrative Subpoena be issued to Charter Communications regarding records related to the following IP address:

147.219.156.74 on 10/02/2023 at 9:08 p.m. CST

147.219.156.74 on 10/08/2023 at 9:36 p.m. CST

147.219.156.74 on 10/08/2023 at 9:36 p.m. CST

35. On October 30, 2023, Charter provided the requested records, which indicated that at those dates and times, IP address 147.219.156.74 was assigned to a Charter customer with the following subscriber information:

STEVE ANDEREGG
N6960 BICE AVE
HOLMEN, WI 546367202
STEVEA137@CHARTER.NET
STEVEA137@GMAIL.COM

(608) 769-1451

36. Additionally, according to the information provided by Meta in the CyberTipline reports, the following Facebook/Instagram accounts are linked by device and/or IP address to ACCOUNT 1:

SUSPECT Facebook account:

Name: Steve Anderegg

Mobile Phone: +16087691451 (Verified)

Date of Birth: 07-05-1981

Approximate Age: 42

Email Address: bewolf.geo@yahoo.com (Verified)

Email Address: stevea137@gmail.com (Verified)

Screen/User Name: steve.anderegg

ESP User ID: 529690284

Profile URL: <https://www.facebook.com/steve.anderegg>

SUSPECT Instagram account:

Instagram Full Name: Dom

Instagram Username: _dhyana_gg

Instagram UID: 55017690550

DOB: July 6 2009

Age: 14

Gender: Unknown

Associated E-Mail Address: None

Associated Phone Number: +16087691451

37. The _dhyana_gg Instagram account (ACCOUNT 2) was referenced in another CyberTipline report numbered 138694255 based on information Instagram reported to NCMEC on November 12, 2022. According to this report, ACCOUNT 2 received an image from another Instagram account via direct message on or about November 9, 2022, that Instagram flagged as depicting potential child pornography. According to the report, Instagram did not review this image before submitting the information to NCMEC.

38. Through open-source searching, PPA Cattaneo was able to identify and locate Minor A. On November 22, 2023, the Georgia Bureau of Investigation (GBI) was able to confirm Minor A's identify. GBI SA Trisha Cannon interviewed Minor A on December 18, 2023. Minor A disclosed his date of birth was in 2008 and confirmed his Instagram username was the one in the conversation with ACCOUNT 1. Minor A reported talking through Instagram with an account that had the vanity name "KING AIDEN," who was posting "immoral and illegal" child pornography on KING AIDEN's public Instagram profile. Minor A stated that he discovered KING AIDEN's profile while searching for motorcycle pages in the Instagram search feature. Minor A thought he remembered the KING AIDEN profile as being the same as ACCOUNT 1. KING AIDEN told Minor A that KING AIDEN used the Prodia AI generator⁴ to create AI images. Minor A stated he requested images of "boys in the woods." Minor A stated that KING AIDEN requested images of Minor A, who then sent a completely nude image of himself to KING AIDEN via Instagram's "vanish mode" function.

39. In a subsequent phone call, Minor A told SA Cannon that he believed KING AIDEN and DOM were two separate people. However, based on my training and experience, and the fact that ANDEREGG has used multiple Instagram profiles, I believe they are likely the same person. Moreover, even if they are not the same person, information provided by Instagram shows that someone using ANDEREGG's account

⁴ According to publicly available information, the Prodia AI generator is a free AI image generator that utilizes Stable Diffusion.

sent the apparently AI-generated images described above to Minor A, in violation of federal statute.

40. SA Cannon obtained consent from the juvenile to search his electronic items and located multiple AI generated CSAM images in the deleted folder.

41. I am familiar with Steven Anderegg from a previous investigation in 2019. While reviewing law enforcement observations on the peer-to-peer file sharing network Freenet, I observed activity from an IP address requesting known files of child sexual abuse material. The internet subscriber for the suspect IP address resolved to Steven Anderegg at the SUBJECT PREMISES. The IP address was observed requesting more than 40 files of known CSAM. The files ranged from prepubescent to young pubescent children engaged in sex acts.

42. On April 28, 2020, agents with WI DOJ-DCI served a search warrant at the SUBJECT PREMISES and collected numerous electronic items. During my interview with Anderegg, he admitted to using multiple peer-to-peer platforms to include Freenet. When asked about seeing CSAM online, Anderegg said "nothing really pops into my mind, but obviously there's lots that you can't really tell if they're 16, 19, or 20." Anderegg stated he didn't knowingly download any CSAM that law enforcement observed being requested over the Freenet network and said he was surprised they all came from one IP address, since he often reset, or unplugged and re-plugged his modem. Anderegg also admitted he would typically uninstall Freenet after every use and re-install it when he wanted to use it again but did not admit at any point to intentionally searching for or downloading CSAM.

43. A full forensic exam was completed on Anderegg's devices seized during the search warrant. The examination uncovered two forensic artifacts labeled as "file:///Z:/11yo%20jacks%20off%20cums%20with%20sound.wmv" and "file:///Z:/NEW2009_9yboycum.wmv," both of which contain terms that I know are indicative of CSAM.

44. Files associated with Frostwire (an additional program Freenet users utilize to request files) were also found during the forensic examination, including files titled "Beryle Shirtless Boy Model (Preteen) (Model Promotions)," "David, Noah & Friends (Boy Candid's - UPDATED)," and "Dennis at camp (boy candid's)."

45. On or about January 29, 2024, I applied for and obtained a federal warrant to search and seize certain data from the Instagram account (ACCOUNT 1) described above. After serving this warrant on Instagram, I received a copy of certain data maintained by Instagram associated with ACCOUNT 1, including private messages the user of ACCOUNT 1 exchanged with other Instagram users. During my review of that content, I observed the private-message exchange between the user of ACCOUNT 1 and Minor A described above. My review of that message exchange revealed that, in addition to the two apparently AI-generated images described above, ACCOUNT 1 sent a third image that also appeared to be computer-generated and depicted prepubescent minors exposing their penises to the viewer. This third image depicted what appeared to be three prepubescent boys standing in a row in a wooded area. The boys are all shirtless and wearing tiny shorts. The boy on the left has his erect penis sticking out of his shorts. The boy on the right has his shorts zipped down to expose his penis, which the boy in the middle appears to be gripping with his hand. The boys are clearly

intended to be prepubescent based on their small statures, underdeveloped physiques, and youthful facial features.

46. During my review of ACCOUNT 1's private messages, I also observed an exchange between ACCOUNT 1 and another Instagram user who reported himself to be a 15-year-old male from around October 2023. ACCOUNT 1 discussed sexually explicit topics with this other user, told the user that he likes "looking at" prepubescent and pubescent boys, and generally expresses a sexual interest in minor males. In another private-message exchange from around September 2023, a different user sends ACCOUNT 1 two videos unprompted. The videos appear to depict a pubescent male, based on his general size, facial features, and bodily development, exposing his penis and masturbating. ACCOUNT 1 responds "Thanks, I guess?" In various other private-message exchanges, posts, and comments from 2023, ACCOUNT 1 mentions that he shares AI-generated images of minor boys on an encrypted mobile messaging application called Telegram and that he runs image-generating AI programs on his own computer locally so that he can produce "sexier" images without being "censored" by online AI models.

47. During recent surveillance of his residence, agents observed Anderegg driving a 2018 gray Tesla Model 3 with Wisconsin registration plate 830-NLZ. Anderegg is also the registered owner of a silver 2017 Subaru Crosstrek SUV with Wisconsin registration plate 178-TNW. Both these vehicles are registered to the SUBJECT PREMISES.

48. Based on my training and experience, people often keep cell phones on their person and computers in their vehicles. Additionally, the items we are searching

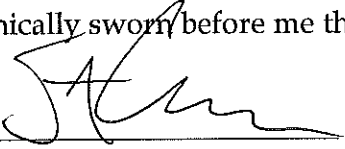
for are very small and portable. Therefore, I request permission to search all
Anderegg's vehicles and person.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search
warrant.

Ryan Condon
Special Agent
WI DOJ-DCI

Telephonically sworn before me this 20th day of February 2024.



Honorable STEPHEN L. CROCKER
Honorable ANDREW R. WISEMAN
United States Magistrate Judge

ATTACHMENT A

1. The property to be searched is N6960 Bice Ave, Holmen, LaCrosse County, Wisconsin further described as a two-story, single-family residence on the east side of the street that faced to the west. The residence had an attached three car garage. The house is covered in a mix of light tan horizontal vinyl siding and light brown/gray brick. The lower third of the garage pillars and entire front porch area have the same brick. The front door is tan and has a thin vertical window to the left of the door. The top of the door has a window shaped in a half-circle. Affixed horizontally to the brick on the pillar to the right of the garage are the numbers "N6960." At the end of the driveway is a green sign affixed to a metal post with the numbers on "N6960" vertically. The roof appears to have brown asphalt shingles. There appears to be one storage shed visible from the road on the property. The shed is located south of the residence and was brown in color.

2. The vehicles to be searched are a 2018 gray Tesla Model 3 with Wisconsin registration plate 830-NLZ and a silver 2017 Subaru Crosstrek SUV with Wisconsin registration plate 178-TNW, both returning to Anderegg's residence.

3. According to Anderegg's driver's license, he is 6'2", weighs 220 pounds, and has brown hair and blue eyes.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography, child erotica, or visual representations of any kind of minors engaged in sexually explicit conduct; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, visual representations of any kind of minors engaging in sexually explicit conduct, or information pertaining to an interest in child pornography, child erotica, or any such visual representations.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the distribution or possession of child pornography, the production, distribution, or possession of explicit material in violation of 18 U.S.C. §1466A, transferring or attempting to transfer obscene material to a minor in violation of 18 U.S.C §1470, or the importation or transportation of obscene matter in violation of 18 U.S.C. §1462(a).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of N6960 Bice Ave, Holmen, WI, by use of the computer or by other means for the purpose of distributing or receiving in any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, or cartoon, computer generated, or artificial intelligence generated child sexual abuse material.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or visual depictions of any kind of minors engaged in sexually explicit conduct, or that cater to those with an interest in child pornography or such depictions.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography or visual depictions of any kind of minors engaging in sexually explicit conduct to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts

with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (electronic storage device) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;
- e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that

are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.